



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/500,869	02/09/2000	Semyon B Mizikovsky		3161

7590 10/02/2003

Docket Administrator (Rm 3C-512)
Lucent Technologies Inc
600 Mountain Avenue P O Box 636
Murray Hill, NJ 07974-0636

EXAMINER

HO, THOMAS M

ART UNIT PAPER NUMBER

2134

DATE MAILED: 10/02/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

3

Office Action Summary

Application No.

09/500,869

Applicant(s)

MIZIKOVSKY, SEMYON B

Examiner

Thomas M Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 2/9/00.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-15 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-15 are pending.

Drawings

2. The examiner objects to the informal drawings filed in this application. While the drawings are sufficient for examination purposes, the examiner requests the applicant to resubmit new formal drawings for Figs 1, 2, 3a, 3b.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1,2, 7-10, 13-14 rejected under 35 U.S.C. 102(e) as being anticipated by Patel, US patent 6,243,811. The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this

Art Unit: 2134

application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

In reference to claim 1:

Patel discloses a method of updating a communications key maintained in a unit for communicating with a communications system, said method comprising:

- generating a new communications key using a secret value stored in said unit, in Patel (column 4, lines 58-62) where the new communications key is the SSD, the said unit is the AC/HLR, and the secret value is the A-Key.

The examiner takes official notice that the Shared Secret Data is understood to be a key for use in mobile communications in the art. (Patel column 1, lines 57-60)

- generating an update key using said secret value stored in said unit. (Patel column 4, lines 1-6), where the update key is the M-key, and the said unit is the AC/HLR.
- performing an authentication using said update key (Patel column 4, lines 43-57), where the authentication is performed using the M-key in a KCF function.

Art Unit: 2134

- updating said communications key with said new communications key after said authentication. (Patel column 4, lines 20-23), where the purpose of generating a KCF and authenticating is specifically for updating the SSD)

In reference to claim 2:

Patel discloses the method of claim 1 comprising:

- Receiving an update sequence. (Patel column 4, lines 22-25), where the update sequence is SR and the random number Rn transmitted with it.
- Generating said new communications key using a secret value stored in said unit and said sequence, where the unit is the AC/HLR. (Patel column 4, lines 58-62)
- Generating a signature value using said update key. (Patel column 4, lines 43-47), where the signature value is the calculation resulting from the KCF function, and the update key, M-key is used as a parameter in the function.
- Comparing said signature value with a signature value received from said communications system which was generated using said update key to perform said authentication. (Patel column 4, lines 43-57), where the signature value received from said communications system is the KCF calculation, generated by M-key, received from the mobile.

In reference to claim 7:

Patel discloses a method of updating a communications key maintained in a unit and in a communications system comprising:

- Sending to said unit, an update sequence for said unit to generate a new communications key using a secret value in said unit. (Patel column 4, lines 20-24, 58-62), where the unit is the mobile unit, the update sequence is SR and the information transmitted with it Rn, the new communications key is SSD, and the SSD is generated by the request SR and Rn after authentication.
- Sending to said unit a signature value for said unit to compare said signature value generated at said communications system using an update key derived from a secret value stored in said communications system associated with said unit. (Patel column 4, lines 48-50), where the signature value is the KCF generated at the communications system AC/HLR, the update key was M-key.
- Receiving an update confirmation after which said communications key is updated with said authentication. (Patel column 4, lines 51-62), where the update confirmation is the authentication, and the update of the SSD thereby proceeds.

In reference to claim 8:

Patel discloses a method comprising:

- Generating said signature value. (Patel column 4, lines 48-50), where the signature value is the KCF generated at the AC/HLR

In reference to claim 9:

Patel discloses a method comprising:

- Receiving a challenge sequence from said unit (Patel column 4, lines 25,26, 43), where the challenge sequence R_m , is generated in the mobile unit and received at the AC/HLR.
- Generating said signature value using said challenge sequence and said update key (Patel column 4, lines 48-50) where the signature value is the KCF, the update key is M-Key, and the challenge sequence is R_m , and the KCF is generated using those values as parameters.

In reference to claim 10:

Patel discloses a method comprising

- Generating a second signature value using said update sequence and said update key (Patel column 4, lines 24-32), where the second signature value is the KCF computed by the mobile unit to authenticate the network.
- Receiving a second signature value generated at said unit using said update sequence and said update key at said unit. (Patel column 4, lines 43-47), where the second signature value is received by the AC/HLR, and the second signature

value was originally generated at the mobile using M-key and Rn from the update sequence.

In reference to claim 13:

Patel discloses a method comprising:

- Generating an update sequence (Patel column 4, lines 20-23), where the update sequence SR and the random value Rn transmitted with it.
- Generating a new communications key using a secret value stored in said communications system and associated with said unit and said update sequence. (Patel column 4, lines 58-62), where the new communications key is the SSD, and the secret value is the A-key.
- Generating an update key using said secret value and said update sequence. (Patel column 4, lines 9-11), where the update key is the M-key, the secret value is the A-key, and the update sequence contains the random number used to generate the M-key through a pseudo random function.
- Updating said communications key with said new communications key after an authentication is performed with said unit using said update key. (Patel column 4, lines 20-24, 58-62), where the new communications key is the SSD generated after authentication is successful.

In reference to claim 14:

Art Unit: 2134

Patel discloses a method comprising:

- Providing said update key to generate a signature value using said update key in said communications system to compare at said unit said signature value with a signature value generated at said unit using an update key generated at said unit using said update sequence and a secret value stored in said unit (Patel column 4 lines 53-57), where the update key(M-key) is used to generate the signature value (the KCF function), at the AC/HLR which is then compared at the mobile unit to the signature values generated at a unit using Mkey generated by the secret value A-key, and the update sequence containing the random number.
- Updating said communications key with said new communications key after receiving the results of said comparison of said signature results. (Patel column 4, lines 20-24, 58-62), where the new communications key is the SSD generated after authentication is successful.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 3-6,11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patel and RFC 2104.

In reference to claim 3:

Patel discloses a method further comprising:

- Generating a challenge sequence. (Patel column 4, lines 20-21)

The examiner takes official notice that a challenge sequence is known in the art to be a random number used in authentication, especially when used as parameters to cryptographic function. (Patel column 2, lines 54-55)

- Sending said challenge sequence to said communications system (Patel column 4, lines 22-23), where the communications system is the mobile.
- Generating said signature value using said challenge sequence and said update key (Patel column 4, lines 29-30)
- Comparing said signature value with said signature value generated by said communications system, where the communications system is the mobile unit. (Patel column 4, lines 44-48)

Patel however fails to disclose: Receiving a signature string generated by said communications system using said challenge sequence and said update key.

Instead Patel(column 4, lines 23-32) discloses that the communications system produces a KCF function or "signature value", whose input parameters comprise an update key(M-key), and challenge sequences Rn and Rm.

Patel(column 4, lines 30-31) additionally reveals that in a preferred embodiment, the KCF function or the "signature value", produced by the mobile unit is preferably a keyed message authentication code such as HMAC. It is therefore necessary that the HMAC also accept as parameters, the update key and challenge sequences, if the HMAC function is to be used as the algorithm for the KCF function.

HMAC is a well known mechanism for message authentication using cryptographic hash functions and is disclosed in RFC 2104. It is known that to compute HMAC we perform

$$H(K \text{ XOR opad}, H(K \text{ XOR ipad}, \text{text}))$$

where H is a cryptographic hash function such as MD5, opad and ipad are typically preset values, K is a secret key, and text is the digital data to be hashed.

H(K XOR ipad, text), specifically is an intermediate value or "signature string" that is produced using K, such as the update key(M-key), and digital data text, which may be supplied the challenge sequences Rm and Rn. It is inherent to the computation of

HMAC that the intermediate value or "signature string" be computed prior to the final computation of the HMAC which is the "signature value".

The examiner takes official notice that the computation of the intermediate value or signature string, based on the challenge sequence R_m , the challenge sequence R_n (which is also a part of the update sequence), and the update key (M-key) is therefore inherent to the preferred embodiment of Patel.

The examiner takes official notice that it is well known in the art that the computation of an algorithm may be divided into portions, where different subparts of the algorithm may be individually computed and then combined together to increase the overall efficiency. For example, RFC 2104 (page 4) shows that the computation of the B-byte blocks may be divided and computed apart from the rest of the algorithm

"These [B-byte blocks] intermediate results are stored and then used to initialize the IV (initial value) of H each time that a message needs to be authenticated... such as savings may be significant when authenticating short streams of data"

It would have been obvious to one of ordinary skill in the art at the time of invention, to send the generated signature string and have it received by another entity where its computation may be completed, given the advantage of increasing efficiency.

In reference to claim 4:

Patel further discloses a method comprising:

- Generating a second signature value using said update sequence and said update key. (Patel column 4, lines 48-50)
- Sending said second signature value to said communications system for comparison with a second signature value generated by said communications system using said sequence and said update key generated at said communications system. (Patel column 4, lines 50-57)

In reference to claim 5:

The development of a signature string comprising at least portions of the update sequence(R_n), said challenge sequence(R_n or R_m), and said update key(M-key) and the generation of the signature value from the signature string is inherent to Patel in the computation of the Keyed Cryptographic Function using the HMAC algorithm as set forth above.

In reference to claim 6:

The development of a second signature string comprising at least portions of the update sequence(R_n), said challenge sequence(R_n or R_m), and said update key(M-key) and the generation of the second signature value from the second signature

Art Unit: 2134

string is inherent to Patel in the computation of the second Keyed Cryptographic Function using the HMAC algorithm as set forth above.

Claims 11 and 12 are rejected for the same reasons as claims 5 and 6 respectively.

7. Claims 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Patel.

Patel discloses the following aspects of claim 15:

- Receiving an update sequence from said home communications system for said unit to generate a new communications key using a secret value in said unit.
(Patel column 4, lines 20-24), where the new communications key is the SSD, and the update sequence is SR and the random number Rn transmitted with it.
- Performing an authentication with said unit using said update sequence (Patel column 4, lines 43-48), where the authentication is done using KCF, which uses Rn from the update sequence.
- Sending to said home communications system the results of said authentication.
(Patel column 4, lines 58-62), where it is inherent that mobile, sends the results of the authentication to the home communications system AC/HLR, before the AC/HLR can begin to generate the new SSD.

Patel however fails to disclose

"Receiving an update key from said home communications system and generated at said home communications system using a secret value associated with said unit at said home communications system."

The update key, M-key is not sent out from the home communications system, AC/HLR, but rather is generated by information provided by the AC/HLR to the mobile.

However, it would have been obvious to one of ordinary skill in the art at the time of invention to send out the update key M-key instead of generating it at the mobile unit as an additional means of having the mobile ultimately acquire the M-key for use in its cryptographic functions.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Art Unit: 2134

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

September 17th, 2003


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100